BURKE COUNTY SHERIFF'S OFFICE
225 HWY 24 SOUTH
WAYNESBORO, GA 30830
(706) 554-2133 FAX (706) 554-3423

REQUEST FOR BIDS

Date Issued: 05/26/2022

THE BURKE COUNTY SHERIFF'S OFFICE IS ACCEPTING SEALED BIDS FROM EXPERIENCED AND QUALIFIED VENDORS FOR IT AND MANAGED CYBERSECURITY SERVICES AS SPECIFIED BELOW FOR THE SHERIFF'S OFFICE. A CONTRACT WILL BE AWARDED TO THE VENDOR WHOSE BID BEST SATISFIES THE REQUIREMENTS FOR THIS REQUEST AND BEST SERVES THE INTEREST OF BURKE COUNTY SHERIFF'S OFFICE. SEALED BIDS WILL BE ACCEPTED UNTIL 5:00 PM ON MONDAY JULY 11, 2022, EST IN THE BURKE COUNTY BOARD OF COMMISSIONERS OFFICE LOCATED AT 602 N. LIBERTY STREET, WAYNESBORO, GA 30830

Burke County Government reserves the right to reject any or all bids and to waive technicalities and informalities.

BID PACKAGE MUST BE RETURNED IN SEALED ENVELOPE AND CLEARLY MARKED

REQUEST FOR BIDS IT AND MANAGED CYBERSECURITY SERVICES
MONDAY JULY 11, 2022, 5:00 PM EST
ATTENTION: MERV WALDROP

FedEx or UPS Ship to address
602 N. Liberty Street,
Waynesboro, GA 30830 ATTENTION: Merv Waldrop

Needed IT Managed Support Services Approach:

Burke County Sheriff's Office desires Managed IT Services delivery for approximately 70 computer users, 120 computers and 4 servers that provides the primary elements of focus:

- Help Desk Services
- On-site Support
- Infrastructure Support
- Security Operations

We are looking for an MSA company whose staff is trained and specialized in the products and solutions that they support, with each of these major areas of focus requiring dedicated and proactive attention to ensure our operations meets our growth, budget, and proficiency goals.

Help Desk Services

- 100% Windows Critical and Security Patching
- Office 365 expertise, including multi-factor setup and security alert monitoring
- SPAM filtering and Phishing Protection (before it reaches Office365 / Outlook!)
- Proactive Monitoring of Event Logs (e.g., Failed Logon Attempts, Failing Hard Drives)
- Knowledgebase (KB) Documentation and Procedures for New Hires, Terminations, Workstation Setups, etc.

On-Site Support

A personable IT department that visits on-site regularly and helps computer users in-person so that our staff feels like the IT team knows and cares about each of them.

Infrastructure Support

We need strong Security and Up-Time in our network closet and throughout our IT system. We desire that our incoming internet connections (incoming coax) are triple surge protected, that the Internet devices are protected with UPS battery backups, and that the network firewall and switches are kept up to date (semi-annual BIOS/Firmware updates). We desire a Backup and Disaster Recovery (BDR) solution that is best-in-class, ensuring backups are performed hourly, without impacting operations and with snapshots that are then replicated hourly, allowing very granular recovery. On-site Image Manager to spin up a backup instance of our server(s) is needed, ensuring continuity without extended downtime in the event of a server failure. We desire a solution that addresses 4 critical areas of Backup / Disaster Recover as follows:

- Onsite (fast) File Recovery
- Onsite Virtual Boot
- Offsite File Recover – a secondary copy of backed up data replicated offsite.
- Offsite Virtual Boot – ability to run an instance of the server based on the last replicated backup, so that business operations can continue, allowing remote workers to work remotely over VPN.

IT AND MANAGED CYBERSECURITY SERVICES

Additional Infrastructure Support services to include the following:

- Active Directory auditing (old accounts, weak passwords, etc.)
- Assist with Vendor Managements
- Office 365 and SharePoint Recovery Services
- Backup image testing and Virtual Boot confirmations

Security Operations:

Burke County Sheriff's Office desires an ideal balance and ROI from Windows and 3rd-Party Patching, Endpoint Protection / EDR (pre- and post-encryption, for Server and Endpoint Protection), SPAM and Phishing protection, and Firewall Security. Our desired additional Cybersecurity services includes the following:

- Endpoint Remote Monitoring (Labtech RMM)
- SonicWALL Security Services (Gateway Antivirus, Anti-malware, Intrusion Prevention, Botnet and C2 blocking, Geo-Fencing)
- Failed Logons monitoring
- Dark Web monitoring of breached user accounts (for our domain)
- User Training and Phishing Campaigns / Scoring

Needed IT Managed Support Services Approach to Include:

- Unlimited Remote and Onsite Remediation (excludes projects)
- 24/7 Remote Monitoring of equipment for failures
- Windows Critical Hotfix and Security Updates
- Managed Endpoint Detection and Response
- Anti-Ransomware Protection
- SPAM and Phishing Protection
- Internal Security Vulnerability Scanning
- External Security Vulnerability Scanning
- Dark Web Monitoring for compromised credentials
- Managed Backup and Disaster Recovery Solution
- Hourly Image-Based Server Backups
- Offsite Replication of Server Backups
- Ability to Virtualize and Boot Backup Images

IT AND MANAGED CYBERSECURITY SERVICES

Technical Approach Needed to Include:

From a data architecture standpoint, we desire to operate with a system that is Azure AD, Office 365, SharePoint, and OneDrive operated. We desire to eliminate many VMs that are only performing Active Directory authentication, to allow us to move multiple VMs back to a single physical server, simplifying and improving performance and backups/Disaster Recovery. We migrated our last Exchange client to O365 around 2016 and have been migrating smaller clients' file shares to SharePoint and OneDrive for company shares and user shares, respectively.

Regarding network architecture, we desire to utilize SonicWALL Total Secure firewall appliances for ingress and egress protection, Cisco SG-series managed switches for VLANs and MAC filtering, Cisco or Meraki APs for private and guest Wi-Fi, and Dell servers and workstations.

We ideally desire a layered approach to security addresses of all 20 CIS Critical Security Controls for Cyber Defense, a solution starting with SonicWALL security services for gateway AV, Malware, and IDS. Servers and endpoints to run Sentinel One EDR/EPP set to block/quarantine, as well as Labtech for event collection and monitoring. Managed Services solution to include a mail gateway layer (via MX redirection) for SPAM and Phishing protection with URL rewriting and time-of-click URL testing. Internet traffic to be protected with a DNS filtering layer. Backup with a powerful 6-core Image Manager workstation that is onsite, where any of the protected servers/endpoints can be virtually booted in minutes should a failure occur (and at a fraction of the cost of a storage-only Datto).

For additional security measures, we would like the following additional layers beyond what is provided with the Managed Services provision: feeding the syslog data from the above devices into a Splunk SIEM for incident monitoring, implementing a solution for low-impact detection of lateral movement and recon, and monthly or quarterly vulnerability scans. An Executive Overview should be provided during monthly or quarterly business reviews (QBRs).

Mobile Device Management:

For MDM needs, we desire utilization of an MDM cloud-based platform, allowing consistent policy application across iPads, Androids, Windows Laptops and Macs without any additional on-premises equipment.

Annual Hardware Replacement Budget & Related Schedule to Upgrade/Get on Track

Over the past several years, we have accumulated a combination of aging hardware that has not been on an adequate replacement schedule, and experienced neglect in critical patching, system monitoring, and layout maintenance of infrastructure closets. We estimate that we have accumulated an $80K "technology debt" in aging hardware that needs to be immediately addressed this year with a plan over the next 3 years to eliminate that critical debt accordingly. We believe that our annual hardware replacement budget should be an estimated $25K to $30K based upon our present number of 120 computers and 4 servers and other hardware, but we estimate it has been used at less than 67% over the past 2 years, requiring an approximate amount of $36K to be utilized over each of the next 2 years to get our hardware replacement schedule back on track.

STATEMENT OF WORK - SCOPE OF SERVICES

Onboarding Services:

- Uninstall any monitoring tools or other software installed by previous IT consultants.
- Compile a full inventory of all protected servers, workstations, and laptops.
- Uninstall any previous virus protection and install managed antivirus application.
- Install remote support access application on each managed device to enable remote support.
- Configure patch management application and check for missing security updates.
- Uninstall unsafe applications or applications that are no longer necessary.
- Optimize device performance including disk cleanup, antivirus, and spyware scans.
- Review firewall configuration and other network infrastructure devices.
- Review status of battery backup protection on servers and infrastructure devices.
- Review and document current server configurations and status.
- Determine existing backup strategy and status; implement at least onsite and offsite file backups.
- Review password policies and update administrative user and device passwords.

Managed Services:

Supported Services

In general, if an employee computer user is experiencing a job-related technical problem, we need to quickly resolve the issue impeding their work.

Support Hours

Covered support to be Monday through Friday during business hours (8:30 AM to 5 PM), excluding holidays. Support outside of these hours to be provided as needed but is billable.

Supported Users

Supported User employees to be able to email or call to initiate a service request. Covered support is limited to a Supported User on a Supported Workstation connected to a Supported Site using a LOB Application as defined below but need to provide support outside of these parameters so long as it is part of the work requirements.
Supported Sites

Our primary Supported Site location/network segment has a covered Firewall, and all computers are Supported Servers or Supported Workstations. We need provided support for the site's network connectivity and security, and management of supported firewalls, switches, and wireless access points.

Supported Workstations / Servers

Supported Workstations and Servers to be onboarded, and will include, as a minimum, remote management, and monitoring (RMM) agent and provided antivirus protection. Utilization of automation to detect and resolve many common issues, as well as for Patch Management. As a best practice, supported devices are restricted to LOB Applications, and administrative access will be restricted to IT provider staff. As a minimum, Supported Servers will be backed up and replicated off-site.

Unsupported Services

We need a provider who is narrowly focused on providing quality IT support within the monthly and annual budget to maintain the existing environment. As such, everything that isn't described in the Proposal as "Supported" shall be considered unsupported. Common examples of unsupported services include New Equipment that hasn't been onboarded, New Software solutions (such as migrating from QuickBooks to Sage), New Software Add-Ons and Integrations (such as a QuickBooks Payment Sync), Print Services (printer hardware and functionality), Internet Services, Home Computers, Electrical Services, Wi-Fi Services (except Cisco/Meraki that we've implemented), and Phone Services.

Additional Definitions and Descriptions

Help Desk Services

When a request is sent by our Employees by email or by phone, the MSA Help Desk needs to gather information, review prior history, determine the impact and urgency, and schedule a Help Desk resource to the request. As the Help Desk resource addresses the service request, they need to update the ticket and communicate with our employee/the end user.

Desired Severity and Resolution

- Service not available (all users and functions unavailable).
  Response Time < 2 hours, Target Resolution Time < 8 hours

- Significant degradation of service (large number of users or business critical functions affected)
  Response Time < 4 hours, Target Resolution Time < 24 hours

- Limited degradation of service (limited number of users or functions affected, business process can continue). Response Time < 24 hours, Target Resolution Time < 72 hours

- Small service degradation (business process can continue, one user affected).
  Response Time < 48 hours, Target Resolution Time Within 6 days

Support Requests

A Support Request ("Ticket") to be created when an employee/end user emails or calls the Help Desk with the details of a request to have a technician create the Ticket. This request is not complete until a Ticket is created and assigned a resource. To be assigned, a request must include, as a minimum, the following: the affected user and / or system, a description of the symptom(s), and proper contact information. When a Ticket is created, the requestor will receive an email with the Ticket number and summary.

On-Site Support Services

When the Help Desk Team has determined that an onsite visit is needed, a technician will be scheduled to come onsite. The technician will arrive to address the scheduled task and will not be available for additional requests due to our other commitments.

Line-of-Business Applications

There are many applications that a User or Workstation utilizes to perform job duties, and these are generally referred to as Line-of-Business (LOB) applications. LOB applications encompass Windows and MS Office, as well as other industry-specific web sites and software such as QuickBooks and Adobe Acrobat. We require that the MSA provider will keep an updated list of supported and unsupported LOB applications for our Offices. We need the MSA provider to research and troubleshoot and when unable to solve the issue internally, then will attempt to open a support request with the software vendor ("Third Party Support"). If Third Party Support is not available or approved, the software will be considered unsupported. Support Requests for unsupported applications are not included as part of the SOW.

Managed Environment

The Managed Environment is comprised of the Supported Sites, Supported Users, Supported Devices, and LOB Applications. We recognize that this is an ever-changing collection of disparate elements, but we expect that our MSA provider will strive hard to be integral to the employee onboarding and offboarding, as well as the equipment requisition processes to maintain a current list of users and equipment.

Change Requests and Lead Times

We recognize that many change requests (commonly referred to as Moves/Adds/Changes) fall outside of normal problem-solving requests. These should be addressed on a First-Available basis and will need to be scheduled in advance. Common change requests are New Users and New Workstation setups, which should be submitted at least two weeks before the start date, or longer if equipment purchasing is required.

Data Backup & Disaster Recovery:

Managed backup of servers to be listed in the Proposal

- Monitoring of backup system, including offsite replication, and onsite backup appliance
- Troubleshooting and remediation of failed backup disks
- Preventive maintenance and management of imaging software
- Firmware and software updates of backup appliance
- Problem analysis by the network operations team
- Monitoring of backup successes and failures

Backed-Up Servers

Proposal to include all servers for back up.

Backup Frequency

On-site backups will occur no less than daily; offsite backups will replicate no less than daily, Monday through Friday.

Backup Data Security

All backed up data is encrypted in transit via SSL and at rest via 256-bit AES encryption. All facilities housing backed up data implement physical security controls and logs.

Backup Retention

Guaranteed retrieval of the most recent recovery point sent to the backup appliance in a local recovery situation. Guaranteed retrieval of archived data sent to the off-site data center in the prior calendar day.

Recovery of Backed-Up Data

Backup recovery provided up to 8 hours during any 12-month period during business hours to be included. Service beyond 8 hours during any 12-month period, or outside of normal business hours to be billable at hourly rate.